CVE Impact Statement

4 May 2001

Common Vulnerabilities and Exposures (CVE) is a simplified dictionary that aims to provide common names for publicly known vulnerabilities (design flaws) and exposures (risky services). The goals of the CVE service are:

1) to make it easier to share data among network and system administrators using different vulnerability databases and tools;
2) to provide a basis for assessing the security of an organization;
3) to provide a set of criteria for users to compare intrusion detection and security scanning products; and
4) to encourage commercial security product and services organizations to provide more-complete coverage of vulnerabilities and exposures in their products and databases.

CVE fills a critical national need in supporting coordination of tools and databases that are used to manage or analyze cyber incidents.

The content of CVE is the result of a collaborative effort of the cyber community through the CVE Editorial Board. The Editorial Board includes representatives from 31 organizations such as security tool vendors, operating system vendors, academic institutions, government, and other prominent security experts. MITRE established CVE and manages the activities of the Editorial Board.

Impacts

Since May 1999, 1309 common names have been agreed on by the Board, and another 1150 candidate names have been proposed.

Candidate names are added at the rate of about 100 a month: some are new vulnerabilities and some are legacy ones that are still active and important. We’re currently seeing 10-20 new vulnerabilities or exposures reported publicly every week.

MITRE runs a database behind the public list of names that enables a new candidate name to be formulated in a matter of days. This process permits the community to adopt the candidate common name early-on in their discussions and attempts to understand and mitigate the new vulnerability or exposure, while awaiting Editorial Board agreement.

Thirty developers of vulnerability databases and tools have declared that their products will be CVE-compatible (48 products). They have done this because their customers have put a high premium on interoperability. In at least one case, a commercial company made its database CVE compatible because a large contract depended on it.

CVE can be the basis for assessing organizations' security readiness and then become the basis for improving the readiness by providing a list of high priority patches to be applied. In the June 2000 announcement by the SANS Institute of how to eliminate the ten most critical Internet security threats, 68 CVE items are referenced.